

WHAT IS CLAIMED IS:

1                   1.       A method for reconstructing a path taken by undesirable  
2   network traffic through a computer network from a source of the traffic, the method  
3   comprising:

collecting statistics at a plurality of measurement points located within forwarding infrastructure of the computer network; and

analyzing the statistics to reconstruct the path taken by the  
undesirable network traffic through the network from the source of the traffic.

1                    2.        The method as claimed in claim 1 further comprising blocking  
2        undesirable network traffic within the computer network upstream of the points  
3        based on the reconstructed path.

1           3.       The method as claimed in claim 1 wherein the forwarding  
2       infrastructure includes at least one router.

1                   4.       The method as claimed in claim 1 wherein the statistics  
2       include flow-based statistics which provide information related to the same logical  
3       traffic flow.

1                   5.       The method as claimed in claim 1 wherein the statistics  
2       include packet statistics which provide information about a set of packets entering  
3       the forwarding infrastructure.

1                   6.       The method as claimed in claim 1 further comprising  
2       requesting and receiving upstream statistics from forwarding infrastructure of the  
3       computer network upstream the measurement points and wherein the step of  
4       analyzing includes the step of analyzing the upstream statistics to reconstruct the  
5       path taken by the undesirable network traffic.

7. The method as claimed in claim 1 wherein the step of  
analyzing includes the step of extracting profiles from the statistics collected at the

3 plurality of measurement points and comparing the profiles to reconstruct the path  
4 taken by the undesirable network traffic.

1 8. The method as claimed in claim 1 wherein the computer  
2 network is the Internet.

1 9. A system for reconstructing a path taken by undesirable  
2 network traffic through a computer network from a source of the traffic, the system  
3 comprising:

4 collectors for collecting statistics at a plurality of measurement points  
5 located within forwarding infrastructure of the computer network; and  
6 at least one controller in communication with the collectors for  
7 analyzing the statistics to reconstruct the path taken by the undesirable network  
8 traffic through the network from the source of the traffic.

1 10. The system as claimed in claim 9 further comprising means  
2 in communication with the at least one controller for blocking undesirable network  
3 traffic within the computer network upstream of the points based on the  
4 reconstructed path.

1 11. The system as claimed in claim 9 wherein the forwarding  
2 infrastructure includes at least one router.

1 12. The system as claimed in claim 9 wherein the statistics include  
2 flow-based statistics which provide information related to the same logical traffic  
3 flow.

1 13. The system as claimed in claim 9 wherein the statistics include  
2 packet statistics which provide information about a set of packets entering the  
3 forwarding infrastructure.

1 14. The system as claimed in claim 9 further comprising means  
2 for requesting and receiving upstream statistics from forwarding infrastructure of

3 the computer network upstream the measurement points and wherein the at least one  
4 controller analyzes the upstream statistics to reconstruct the path taken by the  
5 undesirable network traffic.

1 15. The system as claimed in claim 9 wherein the controller  
2 extracts profiles from the statistics collected at the plurality of measurement points  
3 and compares the profiles to reconstruct the path taken by the undesirable network  
4 traffic.

1 16. The system as claimed in claim 9 wherein the computer  
2 network is the Internet.

1 17. The method as claimed in claim 1 wherein the undesirable  
2 network traffic includes denial of service attacks.

1 18. The method as claimed in claim 17 wherein the computer  
2 network includes a plurality of service provider networks.

1 19. The system as claimed in claim 9 wherein the undesirable  
2 network traffic includes denial of service attacks.

1 20. The system as claimed in claim 19 wherein the computer  
2 network includes a plurality of service provider networks.